IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Ulrich Emmerling et al.
Serial No.:	10/603,209
Date Filed:	June 25, 2003
Group Art Unit:	2168
Examiner:	Dwivedi, Mahesh H.
Title:	**METHOD FOR AUTHENTICATING A FIRST OBJECT TO AT LEAST ONE FURTHER OBJECT, ESPECIALLY THE VEHICLE TO AT LEAST ONE KEY**

MAIL STOP – APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Further to the notice of appeal submitted on October 19, 2006, and the Notice of Panel Decision from Pre-Appeal Brief Review mailed December 19, 2006, Applicants hereby submit this appeal brief according to §41.37.

APPELLANT'S BRIEF (37 C.F.R. § 41.37)

This brief is submitted in support of appellants' notice of appeal from the decision dated August 28, 2006 of the Examiner finally rejecting claims 1-17 of the subject application.

I. REAL PARTY IN INTEREST

The real party in interest is:

Siemens AG
Wittelsbacherplatz 2
80333 München
GERMANY

by virtue of an assignment by the inventors as duly recorded in the Assignment Branch of the U.S. Patent and Trademark Office.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

The application as originally filed contained a total of 17 claims, wherein claims 1 and 11 were independent. The status of the claims are as follows:

Claims Pending:	1-17
Claims Rejected:	1-17
Claims Allowed:	none
Claims Cancelled:	none
Claims Amended:	1-4 and 11-12
Claims Withdrawn:	none
Claims Objected:	none

Appellants appeal the rejection of claims 1-17 of the present application. These claims are reproduced in attached Appendix.

IV. STATUS OF AMENDMENTS

Applicants amended Claims 1-4, 11-12 in a Response to Office Action filed April 25, 2006. No further amendments were made during prosecution.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for authenticating a first object to at least one further object. (*See, e.g.*, specification, page 1, lines 8-11; and page 4, lines 14-16). The method comprises the steps of:

a) transmitting an item of information (ST) unidirectionally between the first object and the at least one further object, (*See, e.g.*, specification, page 4, lines 17-18; page 5, lines 13-9; page 7, lines 9-21; and page 8, lines 5-8)

b) calculating a computation result (calculated RE) in the relevant receiving object from parts of the transmitted information (ST), (*See, e.g.*, specification, page 4, lines 19-20; page 5, lines 20-24; and page 8, line 16 to page 9, line 2)

c) comparing the calculated computation result (calculated RE) with a computation result (transferred RE) transferred with the information (ST) in the relevant receiving object, (*See, e.g.*, specification, page 4, lines 21-22; page 5, lines 20-24; and page 8, line 24 to page 9, line 2) and

d) authenticating the first object to the at least one further object only if there is a match between the calculated computation result (calculated RE) and transferred computation result (transferred RE), and declaring the computation result (calculated RE) as invalid for further transmissions. (*See, e.g.*, specification, page 4, lines 23-24; page 6, lines 16-19; and page 9, lines 3-19).

Independent claim 11 is directed to a method for authenticating a vehicle to at a key. (*See, e.g.*, specification, page 1, lines 8-11; and page 4, lines 14-16). The method comprises the steps of:

a) transmitting an item of information (ST) unidirectionally between the vehicle and the key, (*See, e.g.*, specification, page 4, lines 17-18; page 5, lines 13-9; page 7, lines 9-21; and page 8, lines 5-8)

b) calculating a computation result (calculated RE) in the key from parts of the transmitted information (ST), (*See, e.g.*, specification, page 4, lines 19-20; page 5, lines 20-24; and page 8, line 16 to page 9, line 2)

c) comparing the calculated computation result (calculated RE) with a computation result (transferred RE) transferred with the information (ST), wherein the comparing is in the key, (*See, e.g.*, specification, page 4, lines 21-22; page 5, lines 20-24; and page 8, line 24 to page 9, line 2) and

d) authenticating the vehicle if there is a match between the calculated computation result (calculated RE) and the transferred computation result (transferred RE), and declaring the computation result (calculated RE) as invalid for further transmissions. (*See, e.g.*, specification, page 4, lines 23-24; page 6, lines 16-19; and page 9, lines 3-19).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner finally rejected claims 1-2, and 11 under 35 USC 102(a) as being anticipated by US 4,509,093 ("*Stellberger*"). However, Applicant believes that independent claims 1 and 11 include limitations neither shown nor suggested by *Stellberger*.

Furthermore, the Examiner finally rejected claims 3-10, and 12-17 as being unpatentable over *Stellberger* in view of U.S. Patent 6,381,699 ("*Kocher*"). However, Applicant believes that independent claims 1 and 11 include limitations neither shown nor suggested by *Stellberger* and, therefore, Claims 3-10 and 12-17 which include all the limitations of independent Claims 1 and 11, respectively, cannot be rendered obvious.

VII. ARGUMENT

Claims 1 and 11

The Examiner finally rejected claims 1 and 11 under 35 USC 102(a) as being anticipated by *Stellberger*. The Examiner particularly stated that *Stellberger* teaches:

Step a) of independent method claim 1 and 11 in column 6, lines 60-67 to column 7, lines 1-8 (hereinafter "citation I");

Step b) in column 7, lines 9-23 (hereinafter "citation II");

Step c) in column 4, lines 22-27 (hereinafter "citation III") and column 9, lines 32-36 (hereinafter "citation IV"); and

Step d) in column 5, lines 29-31 (hereinafter "citation V"). Applicants respectfully disagree.

Applicant respectfully disagrees. *Stellberger* generally discloses two different methods of authentication. The first method is graphically represented in Fig. 2 of *Stellberger* and the second method in Fig. 3 of *Stellberger*. These methods are each distinct in their functionality and, thus, the respective steps of these method cannot simply be mixed or interchanged without compromising the functionality of the methods.

Fig. 2 of *Stellberger* represents a method in which upon exitation (step B), a first item of information X is sent from the lock unit 20 to the key unit 10 (step D). Key unit 10 then calculates result Y, Y^{-} (step G) and transmits this result to lock unit 20 which then performs a comparison (step K). Thus, this method clearly differs from the claimed method because the computed result is transmitted before comparison.

The second method shown in Fig. 3, differs from the first method in providing parallel computation and comparison, i.e., both units perform a computation and comparison with items of information transferred from the respective other unit. However, to this end, the second method requires a bidirectional transfer of information.

In the rejection, the Examiner impermissibly identifies different steps of the two *Stellberger* methods and mixes these steps to create a new method which is not disclosed or suggested in *Stellberger*. For example, citations I, II, and V relate to the first method shown in Fig. 2. However, citation III and IV clearly refer to the second method as shown in Fig. 3.

The Examiner impermissible randomly singles out a step of the second method and tries to combine it with the first method. However, such a analysis/conclusion is neither supported by 35 USC §102 or §103. As discussed above, first and second methods perform different steps that cannot be interchanged.

For example, if according to *Stellberger's* first method shown in Fig. 2, step D is regarded as step a) of Claims 1 and 11, then lock unit 20 represents the first object and key unit 10 represents the at least one further object. However, the comparison which is performed in step K of *Stellberger* is also performed in the lock unit 20. Thus, *Stellberger's* first method cannot anticipate Claims 1 and 11.

If according to *Stellberger's* second method shown in Fig. 3, step D_n is regarded to be equivalent to step a) of Claims 1 and 11, then again lock unit 20 represents the first object and key unit 10 represents the at least one further object. In step D_n lock unit 20 transmits information $Z'_1 \ldots Z'_n$ to key unit 10. Key unit 10 then computes a result Y_1 , $\overline{Y}_1$ in step G_1 and H_1. However, the method step c) of Claims 1 and 11 requires that the calculated result is compared to a computation result which has been transferred in the item of information in step a). However, *Stellberger* teaches to perform another separate transmission step J1 to transfer the comparison result $\overline{Y}_1$ from lock unit 20 to key unit 10. Moreover, to be able to calculate this result $\overline{Y}_1$ in lock unit 20, the method of *Stellberger* needs to perform a bidirectional transfer in step D_n in which information is transferred from key unit 10 to lock unit 20 and vice versa. Thus, the second method does neither disclose step a) nor step c) of independent Claim 1 and 11.

In summary, *Stellberger* does not disclose or suggest the specific steps as defined in the independent Claims 1 and 11.

Dependent Claims 2-10 and 12-17

Claim 2 stands rejected as being anticipated by *Stellberger* under 35 U.S.C. §102. Claims 3-10 and 12-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Stellberger* in view of *Kocher*. Applicants respectfully submit that the dependent Claims are allowable at least to the extent of the independent Claim to which they refer, respectively. Because, Claims 1 and 11 are not anticipated by *Stellberger*, the dependent Claims 2-10 and

12-17 cannot be anticipated or rendered obvious by *Stellberger*. Thus, Applicants respectfully request reconsideration and allowance of the dependent Claims.

SUMMARY

Applicants hereby authorize the Commissioner to charge the $500.00 filing fee, and any other fees necessary, or credit any overpayment, to Deposit Account No. 50-2148 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P. (31625)

Date: February 20, 2007

By: 

Andreas Grubert
1500 San Jacinto Center
98 San Jacinto Blvd.
Austin, Texas 78701-4287
Telephone: 512.322.2545
Facsimile: 512.322.8383
ATTORNEY FOR APPELLANTS

VIII. CLAIMS APPENDIX

Claims:

1. (Previously Presented) Method for authenticating a first object to at least one further object-comprising the steps of:

a) transmitting an item of information unidirectionally between the first object and the at least one further object,

b) calculating a computation result in the relevant receiving object from parts of the transmitted information,

c) comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object, and

d) authenticating the first object to the at least one further object only if there is a match between the calculated computation result and transferred computation result, and declaring the computation result as invalid for further transmissions.

2. (Previously Presented) Method in accordance with Claim 1, wherein the first object comprises a vehicle and the at least one further object comprises a key, and wherein the information is transmitted from the vehicle and received by the key.

3. (Previously Presented) Method in accordance with Claim 1, wherein the information comprises: a random number and an incremental or decrementable item of data, wherein the incremental or decrementable item of data is stored in the at least one further object if the calculated computation result matches the transferred computation result, and wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted.

4. (Previously Presented) Method in accordance with Claim 2, wherein the information comprises: a random number and an incremental or decrementable item of data, wherein the incremental or decrementable item of data is stored in the key if the calculated computation result matches the transferred computation result, and wherein after each

transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted.

5. (Original) Method in accordance with Claim 1, wherein a counter state or item of time data is transferred as the item of data that can be incremented.

6. (Original) Method in accordance with Claim 2, wherein a counter state or item of time data is transferred as the item of data that can be incremented.

7. (Original) Method in accordance with Claim 5, wherein the result is only calculated when the transferred item of data is greater than the stored item of data.

8. (Original) Method in accordance with Claim 5, wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid.

9. (Original) Method in accordance with Claim 7, wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid.

10. (Original) Method in accordance with Claim 1, wherein the result is computed in at least one further object using a cryptological computation algorithm known there and a code word.

11. (Previously Presented) Method for authenticating a vehicle to at a key comprising the steps of:

a) transmitting an item of information unidirectionally between the vehicle and the key,

b) calculating a computation result in the key from parts of the transmitted information,

c) comparing the calculated computation result with a computation result transferred with the information, wherein the comparing is in the key, and

d) authenticating the vehicle if there is a match between the calculated computation result and the transferred computation result, and declaring the computation result as invalid for further transmissions.

12. (Previously Presented) Method in accordance with Claim 11, wherein the information comprises: a random number and an incremental or decrementable item of data, wherein the incremental or decrementable item of data is stored in the key if the calculated computation result matches the transferred computation result, and wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted.

13. (Original) Method in accordance with Claim 11, wherein a counter state or item of time data is transferred as the item of data that can be incremented.

14. (Original) Method in accordance with Claim 13, wherein the result is only calculated when the transferred item of data is greater than the stored item of data.

15. (Original) Method in accordance with Claim 13, wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid.

16. (Original) Method in accordance with Claim 14, wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid.

17. (Original) Method in accordance with Claim 11, wherein the result is computed in the key using a cryptological computation algorithm known there and a code word.

IX. EVIDENCE APPENDIX

NONE

X. RELATED PROCEEDINGS APPENDIX

NONE